

T S2/5/1

2/5/1

DIALOG(R) File 351:Derwent WPI
(c) 2005 Thomson Derwent. All rts. reserv.

013608276

WPI Acc No: 2001-092484/200111

XRPX Acc No: N01-069981

Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not

Patent Assignee: RICOH KK (RICO)

Inventor: KANAI Y; YACHIDA M

Number of Countries: 002 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111 B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
DE 10024753	A1	159	G06F-012/14	
JP 2000339223	A	29	G06F-012/14	
JP 2001005728	A	46	G06F-012/14	
JP 2001147898	A	11	G06F-015/00	
JP 2001154577	A	12	G09C-001/00	
JP 2001209582	A	18	G06F-012/14	
JP 2001209581	A	16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06;
G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-339223

(P2000-339223A)

(43)公開日 平成12年12月8日 (2000.12.8)

(51)Int.Cl.⁷
G 0 6 F 12/14
// G 0 9 C 1/00

識別記号
3 1 0
6 4 0

F I
G 0 6 F 12/14
G 0 9 C 1/00

テ-マ-ト^{*} (参考)
3 1 0 A 5 B 0 1 7
6 4 0 D 5 J 1 0 4
9 A 0 0 1

審査請求 未請求 請求項の数 8 O L (全 29 頁)

(21)出願番号 特願平11-145340
(22)出願日 平成11年5月25日 (1999.5.25)

(71)出願人 000006747
株式会社リコー
東京都大田区中馬込1丁目3番6号
(72)発明者 金井 洋一
東京都大田区中馬込1丁目3番6号 株式会社リコー内
(72)発明者 谷内田 益義
東京都大田区中馬込1丁目3番6号 株式会社リコー内
(74)代理人 100089118
弁理士 酒井 宏明

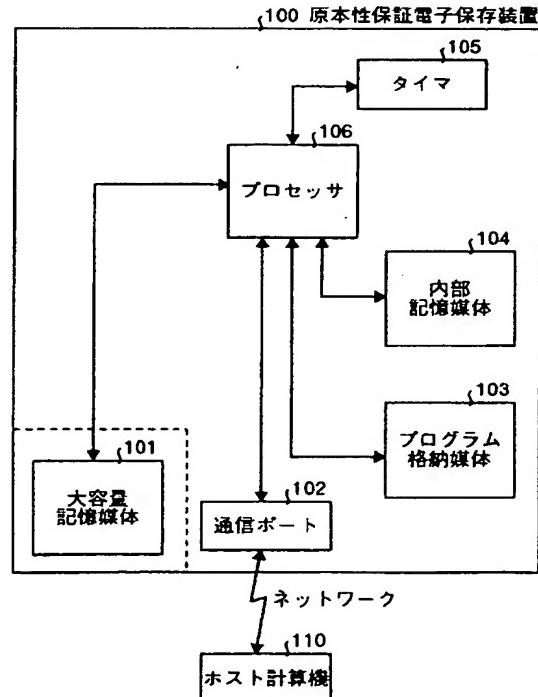
最終頁に続く

(54)【発明の名称】 原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良く行えること。

【解決手段】 複数の版で形成される電子データを一つの原本として識別可能な状態で大容量記憶媒体101に保存しておき、プロセッサ106がこの大容量記憶媒体101の電子データをアクセスする際には、原本とそうでないものとでアクセス制御のレベルを変える。



【特許請求の範囲】

【請求項1】 所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御工程と、を含んだことを特徴とする原本性保証電子保存方法。

【請求項2】 前記保存工程は、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定する第1の改ざん検知情報算定工程と、前記第1の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を生成するデータ属性情報作成工程と、前記データ属性情報作成工程によって作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第2の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程によって算定した改ざん検知情報を前記データ属性情報に付与したデータと、保存対象となる電子データとを前記記憶部に記憶する記憶工程と、を含んだことを特徴とする請求項1に記載の原本性保証電子保存方法。

【請求項3】 前記アクセス制御工程は、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に付与された改ざん検知情報と前記暗号鍵に応答する復号鍵に基づいて、改ざんの有無を検証する第1の改ざん検証工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報から読み出し対象となる版の版管理情報を前記記憶部から読み出す版管理情報読出工程と、前記版管理情報読出工程によって読み出された版管理情報と前記復号鍵に基づいて、改ざんの有無を検証する第2の改ざん検証工程と、前記読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供する提供工程と、を含んだことを特徴とする請求項2に記載の原本性保証電子保存方法。

【請求項4】 外部から原本である電子データの版をバ

- ージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読み出し工程と、前記データ属性情報読み出し工程によって読み出されたデータ属性情報と前記復号鍵に基づいて、改ざんの有無を検証する改ざん検証工程と、新たな版の電子データに前記暗号鍵を適用して該新たな版の電子データの改ざん検知情報を作成する第1の改ざん検知情報算定工程と、前記第3の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報を前記データ属性情報に追加する追加工程と、前記追加工程によって版管理情報が追加されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第2の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程によって算定された改ざん検知情報を前記データ属性情報に付与したデータと新しい版の電子データとを前記記憶部に記憶する記憶工程と、からなるバージョンアップ工程をさらに含んだことを特徴とする請求項2または3に記載の原本性保証電子保存方法。
- 【請求項5】 外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に前記復号鍵を適用して、該データ属性情報の改ざんの有無を検証する第1の改ざん検証工程と、前記複製要求で指定された版の電子データを前記記憶部から読み出す電子データ読出工程と、前記データ属性情報から指定された版の版管理情報を取り出す版管理情報取出工程と、前記版管理情報取出工程によって取り出された版管理情報に前記復号鍵を適用して、改ざんの有無を検証する第2の改ざん検証工程と、前記電子データ読出工程によって読み出された指定された版の電子データを指定された複製先に複製する第1の複製工程と、前記データ属性情報に含まれる属性情報を複写を示す情報に変更する属性情報変更工程と、前記属性変更工程によって属性情報を変更されたデータ属性情報を指定された複製先に複製する第2の複製工程と、からなるデータ複製工程をさらに含んだことを特徴とする請求項2、3または4に記載の原本性保証電子保存方

法。

【請求項6】 外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報を前記データ属性情報に含めて管理することを特徴とする請求項1～5のいずれか一つに記載の原本性保証電子保存方法。

【請求項7】 外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することを特徴とする請求項6に記載の原本性保証電子保存方法。

【請求項8】 前記請求項1～7のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法および記録媒体に関し、特に、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる原本性保証電子保存方法および記録媒体に関する。

【0002】

【従来の技術】 近年のコンピュータ技術の進展に伴うペーパレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【0003】 たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－， Medical Imaging Technology , Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行 創造的ソフトウェア育成事業およびエレクトロニック・コマース推進事業 最終成果発表会論文集 創造的ソフトウェア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【0004】 かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【0005】

【発明が解決しようとする課題】 しかしながら、これらの従来技術のものは、原本に対する修正または訂正を原本データの追記（差分データ）として取り扱うものであるので、差分が反映された最新または任意の時点の状態

の原本データを取得したいとする外部アプリケーションプログラムの要請に応えることができないという問題がある。

【0006】 すなわち、これらの従来技術は、どこからどこまでが最初に記載された原本データで、どこからが後から追記された原本データであるかを示す情報を原本性保証電子保存装置の外部に提供しないため、かかる外部アプリケーションプログラムの要請に応えるために、原本データのバージョン管理を外部アプリケーションプログラム側でおこなわなければならなくなる。

【0007】 また、原本性保証電子保存装置によってCD-Rなどのリムーバブルメディアに原本データを記録した場合には、このリムーバブルメディアを他のドライブ装置を用いて読み出せることができ readability の観点から見て望ましいが、かかる原本性保証電子保存装置によって記録された原本データは、原本性保証電子保存装置に固有なフォーマットで記録されるため、原本データを作成した外部アプリケーションプログラムがデータを直接解読できないという問題もある。

【0008】 さらに、これらの従来技術では、原本データと該原本データを複製した謄本データとを区別して管理する場合に、原本データの内容全体を謄本データとしていたため、かりに最新の原本データのみが必要であっても、この最新の原本データだけではなく過去の原本データが不要をも含めた内容を全て謄本データに保持せねばならず、記録容量の観点から見て効率的ではないという問題もある。なお、原本データから最新の原本データのみを複製した場合には、この複製データはもはや謄本データではなく、その複製データと原本データの関連は保証されない。

【0009】 これらのことから、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理をいかに効率良くおこなうかが極めて重要な課題となっている。

【0010】 この発明は、上記問題（課題）に鑑みてなされたものであり、複数のバージョンからなる原本データを管理する場合に、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる原本性保証電子保存方法および記録媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】 上記目的を達成するためには、請求項1の発明に係る原本性保証電子保存方法は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうア

クセス制御工程と、を含んだことを特徴とする。

【0012】この請求項1の発明によれば、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる。

【0013】また、請求項2の発明に係る原本性保証電子保存方法は、前記保存工程は、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定する第1の改ざん検知情報算定工程と、前記第1の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成するデータ属性情報作成工程と、前記データ属性情報作成工程によって作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第2の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程によって算定した改ざん検知情報を前記データ属性情報に付与したデータと、保存対象となる電子データとを前記記憶部に記憶する記憶工程と、を含んだことを特徴とする。

【0014】この請求項2の発明によれば、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成し、作成されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定し、算定した改ざん検知情報をデータ属性情報に付与したデータと保存対象となる電子データとを記憶部に記憶することとしたので、改ざん検知情報を含むデータ属性情報を電子データとともに記憶することができる。

【0015】また、請求項3の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に付与された改ざん検知情報と前記暗号鍵に応答する復号鍵とに基づいて、改ざんの有無を検証する第1の改ざん検証工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報から読み出し対象となる版の版管理情報を前記記憶部から読み出す版管理情報読出工程と、前記版管理情報読出工程によって読み出された版管理情報と前記復号鍵とに基づいて、改ざんの有無を検証

する第2の改ざん検証工程と、前記読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供する提供工程と、を含んだことを特徴とする。

【0016】この請求項3の発明によれば、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に付与された改ざん検知情報と暗号鍵に応答する復号鍵とに基づいて改ざんの有無を検証し、読み出されたデータ属性情報から読み出し対象となる版の版管理情報を記憶部から読み出し、読み出された版管理情報と復号鍵とに基づいて改ざんの有無を検証し、読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供することとしたので、改ざんを防止しつつ外部に電子データを提供することができる。

【0017】また、請求項4の発明に係る原本性保証電子保存方法は、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を

前記記憶部から読み出すデータ属性情報読み出し工程と、前記データ属性情報読み出し工程によって読み出されたデータ属性情報と前記復号鍵とに基づいて、改ざんの有無を検証する改ざん検証工程と、新たな版の電子データに前記暗号鍵を適用して該新たな版の電子データの改ざん検知情報を作成する第1の改ざん検知情報算定工程と、前記第3の改ざん検知情報算定工程によって算定された改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程によって作成された版管理情報を前記データ属性情報に追加する追加工程と、前記追加工程によって版管理情報が追加されたデータ属性情報に前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定する第2の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程によって算定された改ざん検知情報を前記データ属性情報に付与したデータと新しい版の電子データとを前記記憶部に記憶する記憶工程と、からなるバージョンアップ工程をさらに含んだことを特徴とする。

【0018】この請求項4の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出し、読み出されたデータ属性情報と復号鍵とに基づいて改ざんの有無を検証し、新たな版の電子データに暗号鍵を適用して該新たな版の電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報を前記データ属性情報に追加する追加工程と、追加されたデータ属性情報に暗号鍵を適用して該データ属性情報の改ざん検知情報を算定し、算定された改ざん検知情報をデータ属性情報に付与した

データと新しい版の電子データとを記憶部に記憶することとしたので、改ざんを防止しつつ効率良くバージョンアップをおこなうことができる。

【0019】また、請求項5の発明に係る原本性保証電子保存方法は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を前記記憶部から読み出すデータ属性情報読出工程と、前記データ属性情報読出工程によって読み出されたデータ属性情報に前記復号鍵を適用して、該データ属性情報の改ざんの有無を検証する第1の改ざん検証工程と、前記複製要求で指定された版の電子データを前記記憶部から読み出す電子データ読出工程と、前記データ属性情報から指定された版の版管理情報を取り出す版管理情報取出工程と、前記版管理情報取出工程によって取り出された版管理情報に前記復号鍵を適用して、改ざんの有無を検証する第2の改ざん検証工程と、前記電子データ読出工程によって読み出された指定された版の電子データを指定された複製先に複製する第1の複製工程と、前記データ属性情報に含まれる属性情報を複写を示す情報に変更する属性情報変更工程と、前記属性変更工程によって属性情報が変更されたデータ属性情報を指定された複製先に複製する第2の複製工程と、からなるデータ複製工程をさらに含んだことを特徴とする。

【0020】この請求項5の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に復号鍵を適用して、該データ属性情報の改ざんの有無を検証し、複製要求で指定された版の電子データを記憶部から読み出し、データ属性情報から指定された版の版管理情報を取り出し、取り出された版管理情報に復号鍵を適用して改ざんの有無を検証し、指定された版の電子データを指定された複製先に複製し、データ属性情報に含まれる属性情報を複写を示す情報に変更し、変更されたデータ属性情報を指定された複製先に複製することとしたので、改ざんを防止しつつ効率良く電子データを複製することができる。

【0021】また、請求項6の発明に係る原本性保証電子保存方法は、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報を前記データ属性情報に含めて管理することを特徴とする。

【0022】この請求項6の発明によれば、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報をデータ属性情報に含めて管理することとしたので、差分データとして電子データを管理する場合であっても効率良く版管理することができる。

【0023】また、請求項7の発明に係る原本性保証電

子保存方法は、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することを特徴とする。

【0024】この請求項7の発明によれば、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することとしたので、差分データで電子データを管理する場合であっても、さらに効率良く版管理をおこなうことができる。

【0025】また、請求項8の発明に係る記録媒体は、前記請求項1～7のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項1～7の動作をコンピュータによって実現することができる。

【0026】

20 【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0027】図1は、本実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示すように、この原本性保証電子保存装置100は、原本となる電子データを記憶し、ネットワークを介してホスト計算機110からアクセスされる装置であり、大容量記憶媒体101と、通信ポート102と、プログラム格納媒体103と、内部記憶媒体104と、タイマ105と、プロセッサ106とからなる。

30 【0028】大容量記憶媒体101は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやCD-Rなどからなる。通信ポート102は、ネットワークを介したホスト計算機との通信をおこなうためのインターフェース部であり、たとえばLANカードなどの通信モジュールなどからなる。

40 【0029】プログラム格納媒体103は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なEEPROMや読み出し専用のROMなどからなる。

【0030】内部記憶媒体104は、各種プログラムの実行に必要となるパラメータを記憶するEEPROMなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。タイマ105は、プロセッサ106がプログラムの実行時に

50 所得する時刻を計時するタイマである。

【0031】なお、大容量記憶媒体101については、図中に破線で示したように原本性保証電子保存装置100から取り外し可能としても良いが、その他の構成部についても原本性保証電子保存装置100と物理的に一体化し、通信ポート102以外からのアクセスを受け付けない耐タンパー性を有する構成にする。ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【0032】プロセッサ106は、プログラム格納媒体103に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行する制御装置である。

【0033】具体的には、このプロセッサ106は、ユーザから保存要求のあったデータを大容量記憶媒体101に保存する際に、あとでデータの改ざんを検出できるようにするために、内部記憶媒体104に記憶したプライベートキーを用いて保存するデータにメッセージ認証子を附加する。なお、このメッセージ認証子は、たとえば公開鍵暗号方式を採用した場合には、デジタル署名として付加するデータに該当する。

【0034】また、データそのものの不正な抹消を検出するために、大容量記憶媒体101に記憶されているデータのリストに対してもメッセージ認証子を付加し、さらにたとえば大容量記憶媒体101の状態を過去の状態に戻すような不正なすり替えを検出するために、大容量記憶媒体101の媒体識別番号と、その媒体のデータリストに対するメッセージ認証子の対を内部記憶媒体104に記憶して管理する。

【0035】また、データ作成日などを不正に変更することができないように、タイマ105から現在時刻を取得し、この時刻をデータの属性として付与とともに、原本性保証電子保存装置100内部でオリジナルな電子データである原本データとそのコピーとを区別することができるよう、「仮原本」、「原本」および「謄本」といった属性をデータに付与して管理する。たとえば、「原本」という属性が付与されたデータコピーした場合には、このコピーしたデータに「謄本」という属性が付与される。

【0036】なお、この属性は外部から変更することはできず、また大容量記憶媒体101を取り外して外部にてその属性を改ざんしたとしても、この大容量記憶媒体101を装置に装着した際に改ざんの有無を検出する。

【0037】次に、図1に示した原本性保証電子保存装置100による新規データの保存処理について図2および図3を用いて説明する。図2は、図1に示した原本性保証電子保存装置100による新規データの保存処理手順を示すフローチャートであり、図3は、この原本性保

証電子保存装置100による新規データの保存処理の概念を説明するための説明図である。

【0038】図2および図3に示すように、大容量記憶媒体101がマウントされている場合には、通信ポート102を介してユーザからデータ、データ属性コードおよびデータ名を受け取る（ステップS201）。具体的には、図3に示す「原本」などがデータ属性コードに該当し、「FileA.doc」などがデータ名に該当する。そして、受け取ったデータ属性コードが「原本」、「仮原本」または「一般」のいずれでもなければ、エラー処理をおこなう。

【0039】これに対して、このデータ属性コードが「原本」、「仮原本」または「一般」のいずれかであれば、データ属性コードが「一般」であるか否かを判断し（ステップS202）、「一般」である場合には（ステップS202肯定）、受け取ったデータを受け取ったデータ名で保存して処理を終了する（ステップS203）。

【0040】一方、このデータ属性コードが「一般」でない場合には（ステップS202否定）、初版としてバージョン属性情報の作成処理をおこなう（ステップS204）。具体的には、受け取ったデータに対してハッシュ値を計算し、ハッシュ値を装置暗号鍵で暗号化してメッセージ認証子（バージョンMAC）とし、内部記憶媒体104より最新のタイマIDを取得し、初版でない場合には、受け取ったバージョンアップモードをデータファイルタイプとし、対象データのバージョン番号、現在時刻、タイマID、対象データを保存する際のファイル名、データファイルタイプ、対象データのサイズおよびバージョンMACなどを含むバージョン属性情報を作成するという手順でバージョン属性情報を作成する。なお、図3に示す例では、「Ver.1 1993.3.27 FileA#1.doc 56KB, MAC」からなるバージョン属性情報を作成した場合を示している。

【0041】その後、この原本性保証電子保存装置100は、データ属性情報を作成処理する（ステップS205）。具体的には、内部記憶媒体104から最新データ識別番号を取得し、最新データ識別番号を1増加させて内部記憶媒体104に記録し、対象データのバージョン属性情報から初版の作成日時情報を取得して作成日時情報を取得して作成日時情報、最終更新日時情報とし、データ属性コード、最新データ識別番号、作成日時情報、最終更新日時情報およびバージョン属性情報などを合わせてデータ属性情報とするという手順でデータ属性情報を作成する。図3に示す例では、「R00012321 原本 1999.3.27 1999.3.27, MAC」というデータ属性情報を作成した場合を示している。

【0042】その後、大容量記憶媒体101から保存データリストファイルを改ざん検知読み出し処理し（ステップS206）、保存データリストに新たなデータのエ

ントリを追加した後に（ステップS207）、受け取ったデータ名にバージョン番号を組み込んだファイル名でデータを大容量記憶媒体101にファイルとして保存し（ステップS208）、データ属性情報を改ざん検知保存処理し（ステップS209）、新しい保存データリストファイルを改ざん検知保存処理した後に（ステップS210）、保存データリストファイルのメッセージ認証子（リストMAC）で内部記憶媒体104の媒体認証コードリストを更新する（ステップS211）。

【0043】具体的には、このデータ属性情報の改ざん検知保存処理では、保存するデータに対してハッシュ値を計算し、ハッシュ値を装置暗号鍵で暗号化し、メッセージ認証子とし、メッセージ認証子とともにデータをファイルとして大容量記憶媒体に保存するという手順の処理をおこなう。

【0044】次に、大容量記憶媒体101のマウント処理について説明する。図4は、図1に示した大容量記憶媒体101のマウント処理手順を示すフローチャートである。同図に示すように、まず最初に装着された大容量記憶媒体101がフォーマットされているか否かを調べ（ステップS401）、フォーマットされていない場合には（ステップS401否定）、大容量記憶媒体101をフォーマットする（ステップS402）。

【0045】具体的には、媒体を初期化し、内部記憶媒体104から媒体認証コードリストを取得し、媒体認証コードリストから最新の媒体識別番号を取得し、媒体識別番号を1増加させた新しい媒体識別番号を大容量記憶媒体101に記録し、内部記憶媒体104の媒体認証コードリストに新しい媒体識別番号のエントリを追加する（リストMACなし）という手順で大容量媒体101をフォーマットする。

【0046】そして、装着された大容量記憶媒体がフォーマット済みの場合（ステップS401否定）またはステップS402によるフォーマット処理を終了した場合には、保存データリストファイルを改ざん検知読み出し処理する（ステップS403）。

【0047】具体的には、対象ファイルを読み出し、対象ファイルに記録されたメッセージ認証子とデータを分離し、データに対してハッシュ値を計算し、内部記憶媒体104から装置暗号鍵を取得し、装置復号鍵でメッセージ認証子を復号して検証用ハッシュ値とし、先のハッシュ値が検証用ハッシュ値と一致しない場合には改ざんされたものと判断する処理をおこなう。

【0048】そして、改ざんがなされていると判断された場合には（ステップS404否定）、エラー処理をおこない（ステップS410）、改ざんがなされていないと判断された場合には（ステップS404否定）、大容量記憶媒体101から媒体識別番号を取得し（ステップS405）、この媒体識別番号に該当するメッセージ認証子（リストMAC）を内部記憶媒体104から取得す

るとともに（ステップS406）、保存データリストファイルに付与されたメッセージ認証子を取得する（ステップS407）。

【0049】そして、両メッセージ認証子が同じであるならば（ステップS408否定）、認証に成功したものとして正常終了し、両メッセージ認証子が異なる場合には（ステップS408肯定）、エラー処理する（ステップS410）。

【0050】上記一連の処理をおこなうことにより、大容量記憶媒体101が取り外し可能な場合に、この大容量記憶媒体101のマウント時にその正当性を検証することができる。

【0051】次に、図1に示した原本性保証電子保存装置100によるデータ読み出し処理について説明する。図5は、図1に示した原本性保証電子保存装置100によるデータ読み出し処理手順を示すフローチャートである。

【0052】同図に示すように、大容量記憶媒体101がマウントされた後に、対象データに関連づけられたデータ属性ファイルが存在しない場合には（ステップS501否定）、対象データファイルを読み出し（ステップS502）、読み出したデータをユーザに送信して（ステップS514）、処理を終了する。

【0053】これに対して、対象データに関連づけられたデータ属性ファイルが存在する場合には（ステップS501肯定）、大容量記憶媒体101の保存データリストファイルから対象データのエントリを取得する（ステップS503）。なお、対象データのエントリが存在しない場合にはエラー処理をおこなう。

【0054】そして、このエントリからデータ属性MACを取得し（ステップS504）、大容量記憶媒体101から対象データのデータ属性情報ファイルを改ざん検知読み出し処理し（ステップS505）、改ざんされている場合にはエラー処理をおこなう（ステップS506）。

【0055】一方、改ざんされていない場合には、取得したデータ属性情報からデータ属性MACを取得し（ステップS507）、取得したデータ属性MACと前のデータ属性MACとが一致しない場合には（ステップS508否定）、エラー処理をおこない（ステップS515）、両者が一致する場合には（ステップS508肯定）、大容量記憶媒体101から対象データの対象バージョンのデータファイルを読み出す（ステップS509）。なお、データファイルが存在しない場合には、エラー処理をおこなう。

【0056】その後、読み出したデータのハッシュ値を計算し（ステップS510）、データ属性情報から対象バージョンのバージョンMACを取得するとともに（ステップS511）、バージョンMACを装置復号鍵で復号してハッシュ値を取得し（ステップS512）、両ハ

ハッシュ値が異なる場合には（ステップS513肯定）エラー処理をおこない（ステップS515）、両ハッシュ値が一致する場合には（ステップS513否定）、読み出したデータをユーザに送出して（ステップS514）処理を終了する。

【0057】上記一連の処理をおこなうことにより、ユーザからデータを受け取ると、対象データの正当性を検証した後に、該当するデータをユーザに送出することができる。

【0058】次に、図1に示した原本性保証電子保存装置100による謄本作成処理について説明する。図6は、図1に示した原本性保証電子保存装置100による謄本作成処理手順を示すフローチャートである。この原本性保証電子保存装置100では、「原本」の属性を持つデータに対する複製要求を受け取ると、対象データファイルと、それに関連づけられたデータ属性ファイルとを複写し、新たなデータ属性ファイルには「謄本」のデータ属性コードを付加する。

【0059】具体的には、まず最初に対象データのデータ属性ファイルを改ざん検知読み出し処理をし、読み出したデータ属性情報ファイルからデータ属性コードを取得し、データ属性コードが「原本」であることを確認する。なお、バージョン番号が指定されていない場合には対象バージョンを全バージョンとし、対象バージョン番号が-1である場合には、対象バージョンを最新版とし、対象バージョンが全バージョンでない場合には、完全バージョンから指定されたバージョンまでを対象バージョンとする。

【0060】そして、図6に示すように、対象データの対象バージョンに対応するバージョンMACをデータ属性情報から取得し（ステップS601）、このバージョンMACを装置復号鍵で復号してバージョンハッシュ値とし（ステップS602）、対象データの対象バージョンのデータファイルからハッシュ値を計算して（ステップS603）、ハッシュ値が一致するか否かを確認する（ステップS604）。

【0061】その結果、両ハッシュ値が一致しない場合には（ステップS604否定）、エラー処理をおこなって（ステップS605）処理を終了し、両ハッシュ値が一致する場合には（ステップS604肯定）、保存データリストファイルを改ざん検知読み出し処理し（ステップS606）、保存データリストから対象データのデータ属性MACを取得する（ステップS607）。

【0062】そして、このデータ属性MACが一致しない場合には（ステップS608否定）エラー処理をおこない（ステップS605）、データ属性MACが一致する場合には（ステップS608肯定）、作成先が同じ原本性保証電子保存装置であるか否かを調べる（ステップS609）。

【0063】そして、同じ装置内である場合には（ステ

ップS609肯定）、対象データの対象バージョンのデータファイルを作成先にコピーし（ステップS610）、対象データのデータ属性情報ファイルを作成先のデータ属性情報ファイルとしてコピーし（ステップS611）、作成先のデータ属性情報ファイルを改ざん検知読み出し処理する（ステップS612）。

【0064】そして、読み出したデータ属性情報のデータ属性コードを「謄本」に変更し（ステップS613）、読み出したデータ属性情報から対象バージョンのバージョン属性情報を取得して（ステップS614）、バージョン属性情報に含まれるファイル名を新しいファイル名に更新する（ステップS615）。

【0065】そして、タイマ105から現在時刻を取得し（ステップS616）、データ属性情報に謄本作成履歴（アカウント名、現在時刻およびタイマID等）を追加して（ステップS617）、データ属性情報を改ざん検知保存処理する（ステップS618）。

【0066】そして、保存データリストファイルを改ざん検知読み出し処理して（ステップS619）、保存データリストに作成先データのエントリを追加し（ステップS620）、新しい保存データリストを改ざん検知保存処理し（ステップS621）、新しい保存データリストファイルのリストMACを内部記憶媒体104の媒体認証コードリストに記録する（ステップS622）。

【0067】これに対して、作成先が同じ装置内でない場合には（ステップS609否定）、ログイン処理をおこなった後に（ステップS623）、対象データの対象バージョンのデータファイルを読み出し（ステップS624）、読み出しデータを作成先装置に謄本作成モードで転送し（ステップS625）、対象データのデータ属性情報ファイルを改ざん検知読み出し処理する（ステップS626）。

【0068】そして、タイマ105から現在時刻を取得し（ステップS627）、データ属性情報に謄本作成履歴を追加し（ステップS628）、新しいデータ属性情報を作成先の装置に謄本作成モードで転送する（ステップS629）。

【0069】次に、図1に示した原本性保証電子保存装置100のデータ移動処理について説明する。図7および図8は、図1に示した原本性保証電子保存装置100のデータ移動処理手順を示すフローチャートである。なお、図7は、移動先が同じ装置内である場合を示し、図8は移動先が異なる装置である場合を示している。

【0070】まず移動先が同じ装置である場合には、まず最初に作成先のデータがすでに存在する場合にはエラー処理をおこない、また対象データにデータ属性情報ファイルが存在しない場合には、対象データのデータファイルを移動先に移動する。

【0071】そして、図7に示すように、保存データリストファイルを改ざん検知読み出し処理し（ステップS

701)、読み出した保存データリストから対象データに対応するデータ属性MACを取得し(ステップS702)、対象データのデータ属性情報ファイルからデータ属性MACを読み出す(ステップS703)。

【0072】そして、対象データの全データファイルを移動先に移動し(ステップS704)、対象データのデータ属性情報ファイルを移動先に移動した後(ステップS705)、保存データリスト内の移動したファイルのエントリを更新する(ステップS706)。

【0073】そして、新しい保存データリストを改ざん検知保存処理した後に(ステップS707)、新しい保存データリストファイルのリストMACで内部記憶媒体104の媒体認証コードリストを更新する(ステップS708)。

【0074】また、移動先が他の装置である場合には、保存データリストファイルを改ざん検知読み出し処理し(ステップS801)、移動先の装置にログイン処理する(ステップS802)。そして、対象データにデータ属性情報ファイルが存在しない場合には(ステップS803否定)、対象データのデータファイルを大容量記憶媒体101から読み出し(ステップS804)、読み出したデータを移動モードで転送し(ステップS805)、対象データのデータファイルを大容量記憶媒体101から削除して処理を終了する。

【0075】これに対して、データ属性ファイルが存在する場合には(ステップS803否定)、保存データリストファイルを改ざん検知読み出し処理し(ステップS807)、読み出した保存データリストから対象データに対応するデータ属性MACを取得し(ステップS808)、対象データのデータ属性情報ファイルからデータ属性MACを読み出す(ステップS809)。

【0076】そして、データ属性MACが一致しない場合には(ステップS810肯定)、対象データのデータ属性情報ファイルを改ざん検知読み出し処理し(ステップS812)、改ざんされていると判断した場合には(ステップS813肯定)、エラー処理をおこなって(ステップS811)処理を終了する。

【0077】これに対して、改ざんされていない場合には(ステップS813否定)、対象データの全バージョンについてデータファイルを大容量記憶媒体101から読み出し(ステップS814)、読み出したそれぞれのバージョンについてデータのハッシュ値を計算し(ステップS815)、データ属性情報から全バージョンについてバージョンMACを取得し(ステップS816)、取得したそれぞれのバージョンMACを装置復号鍵で復号して検証ハッシュ値を取得する(ステップS817)。

【0078】そして、対応する検証ハッシュ値と先のハッシュ値のうち、異なるものが存在する場合には(ステップS818肯定)、エラー処理をおこなって処理を終

了し(ステップS811)、異なるものが存在しない場合には(ステップS818否定)、タイマ105から現在時刻を取得し(ステップS819)、データ属性情報にデータ移動履歴を追加して(ステップS820)、新しいデータ属性情報を移動先の装置に移動モードで転送する(ステップS821)。

【0079】その後、対象データのデータファイルを全て削除し(ステップS822)、対象データのデータ属性情報ファイルを削除し(ステップS823)、保存データリスト内の移動したデータのエントリを削除し(ステップS824)、新しい保存データリストを改ざん検知保存処理する(ステップS825)。

【0080】そして、新しい保存データリストのリストMACで内部記憶媒体104の媒体認証コードリストを更新し(ステップS826)、作成先装置からログアウト処理をおこなって処理を終了する(ステップS827)。

【0081】次に、異なる原本性保証電子保存装置に上記データ移動処理をおこなう場合の移動先の転送受け入れ処理について説明する。図9は、異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の転送受け入れ処理手順を示すフローチャートである。

【0082】図9に示すように、転送先の原本性保証電子保存装置は、まず最初に転送先データがすでに存在するか否かを確認し(ステップS901)、すでに存在する場合には(ステップS901肯定)、エラー処理をおこなって処理を終了する(ステップS902)。

【0083】これに対して、転送先データが存在しない場合には(ステップS901否定)、謄本作成モードであるか否かを確認し(ステップS903)、謄本作成モードである場合には(ステップS903肯定)、保存データリストファイルを改ざん検知読み出し処理し(ステップS904)、受け取ったデータに対してハッシュ値を計算し(ステップS905)、ハッシュ値を装置暗号鍵で暗号化してバージョンMACとする(ステップS906)。

【0084】そして、受け取ったデータ属性情報の中のバージョンMACを更新し(ステップS907)、データ属性情報のデータ属性コードを「謄本」に変更し(ステップS908)、データ属性情報に謄本作成履歴を追加し(ステップS909)、新しいデータ属性情報を改ざん検知保存処理する(ステップS910)。

【0085】そして、受け取ったデータをデータファイルとして大容量記憶媒体101に保存し(ステップS911)、保存データリストに作成した謄本データのエントリを追加して(ステップS912)、新しい保存データリストを改ざん検知保存処理し(ステップS913)、保存データリストファイルのリストMACで内部記憶媒体104の媒体認証コードリストを更新して(ステップS914)、処理を終了する。

【0086】一方、ステップS903において謄本作成モードではなく移動モードであると判断された場合には（ステップS903否定）、保存データリストファイルを改ざん検知読み出し処理し（ステップS203）、受け取ったデータに対してハッシュ値を計算し（ステップS916）、データ属性情報を受け取ったか否かを確認する（ステップS917）。

【0087】そして、データ属性情報を受け取った場合には（ステップS917肯定）、ハッシュ値を装置暗号鍵で暗号化してバージョンMACとし（ステップS918）、データ属性情報の中のバージョンMACを更新して（ステップS919）、データ属性情報にファイル移動履歴を追加する（ステップS920）。

【0088】そして、新しいデータ属性情報を改ざん検知保存処理し（ステップS921）、受け取ったデータをデータファイルとして大容量記憶媒体101に保存して（ステップS922）、保存データリストに受け取ったデータのエントリを追加する（ステップS923）。

【0089】そして、新しい保存データリストを改ざん検知保存処理し（ステップS924）、保存データリストファイルのリストMACで内部記憶媒体の媒体認証コードリストを更新して（ステップS925）、処理を終了する。なお、上記ステップS917でデータ属性情報を受け取らない場合には（ステップS917否定）、そのまま処理を終了する。

【0090】次に、図1に示した原本性保証電子保存装置100によるデータの削除処理について説明する。図10は、図1に示した原本性保証電子保存装置100によるデータの削除処理手順を示すフローチャートである。同図に示すように、まず保存データリストファイルを改ざん検知読み出し処理し（ステップS1001）、対象データに該当するエントリを取得する（ステップS1002）。

【0091】そして、このエントリが存在しない場合には（ステップS1003否定）、対象データを削除して（ステップS1004）処理を終了し、エントリが存在する場合には（ステップS1003肯定）、データ属性コードが「原本」であるか否かを確認する（ステップS1005）。

【0092】そして、データ属性コードが「原本」である場合には（ステップS1005肯定）、エラー処理をおこなって処理を終了し（ステップS1006）、「原本」でない場合には（ステップS1005否定）、保存データリストから対象データに該当するエントリを削除し（ステップS1007）、新しい保存データリストを改ざん検知保存処理する（ステップS1008）。

【0093】そして、保存データリストファイルのリストMACで内部記憶媒体104の媒体認証コードリストを更新した後（ステップS1009）、対象データのデータファイルを削除し（ステップS1010）、対象デ

ータのデータ属性ファイルをも削除して（ステップS1011）処理を終了する。

【0094】次に、図1に示した原本性保証電子保存装置100によるデータ属性コードの変更処理について説明する。データ保存処理において、「仮原本」の属性を持つデータを保存することはできるが、この「仮原本」データは単純にデータ属性コードを「原本」に変更することが可能である。また、「謄本」、「バックアップ仮原本」、「バックアップ原本」および「バックアップ謄本」の属性を持つデータはそれぞれ属性コードを変更することで元のデータを復旧することができる。かかる復旧をおこなうと、図11に示すように、「謄本」が「原本」に復旧され、「バックアップ仮原本」が「仮原本」に復旧され、「バックアップ原本」が「原本」に復旧され、「バックアップ謄本」が「謄本」に復旧される。なお、かかるデータ属性コードを変更するとこれをデータアクセス履歴として記録することとなる。

【0095】また、図12は、図1に示した原本性保証電子保存装置100によるデータ属性コードの変更処理手順を示すフローチャートである。同図に示すように、まず最初に保存データリストを改ざん検知読み出し処理し（ステップS1201）、保存データリストから対象データに該当するエントリを取得したならば（ステップS1202）、エントリから現属性コードを取得する（ステップS1203）。

【0096】そして、新データ属性コードが「仮原本」であり（ステップS1204肯定）、現データ属性コードが「バックアップ仮原本」である場合には（ステップS1205肯定）、データ属性情報のデータ属性コードを「仮原本」に変更する（ステップS1206）。なお、ステップS1205で現データ属性コードが「バックアップ仮原本」でない場合には（ステップS1205）、エラー処理をおこなって処理を終了する（ステップS1219）。

【0097】また、新データ属性コードが「仮原本」でない場合には（ステップS1204否定）、この新データ属性コードが「原本」であるか否かを調べ（ステップS1207）、この新データ属性コードが「原本」である場合には（ステップS1207肯定）、現データ属性コードが「バックアップ仮原本」または「仮原本」であるか否かを調べ（ステップS1208）、「バックアップ仮原本」または「仮原本」である場合には（ステップS1208肯定）、データ属性情報のデータ属性コードを「原本」に変更する（ステップS1209）。なお、ステップS1208で現データ属性コードが「バックアップ原本」または「仮原本」でない場合には（ステップS1208否定）、エラー処理をおこなって処理を終了する（ステップS1219）。

【0098】また、新データ属性コードが「原本」でない場合には（ステップS1207否定）、この新データ

属性コードが「臍本」であるか否かを調べ（ステップS1210）、この新データ属性コードが「臍本」である場合には（ステップS1210肯定）、現データ属性コードが「バックアップ臍本」であか否かを調べ（ステップS1211）、「バックアップ臍本」である場合には（ステップS1211肯定）、データ属性情報のデータ属性コードを「臍本」に変更する（ステップS1212）。なお、ステップS1211で現データ属性コードが「バックアップ臍本」でない場合には（ステップS1211否定）、エラー処理をおこなって処理を終了する（ステップS1219）。

【0099】そして、これらの変更を終えたならば、タイム105から現在時刻を取得し（ステップS1213）、データ属性情報にデータ属性コード変更履歴を追加して（ステップS1214）、新しいデータ属性情報を改ざん検知保存処理する（ステップS1215）。

【0100】その後、保存データリストの対象データに該当するエントリについて内容を更新し（ステップS1216）、新しい保存データリストを改ざん検知保存処理して（ステップS1217）、保存データリストファイルのリストMACで内部記憶媒体104の媒体認証コードリストを更新して（ステップS1218）、処理を終了する。

【0101】次に、図1に示した原本性保証電子保存装置100によるデータのバージョンアップ処理について説明する。このデータバージョンアップ処理では、「原本」および「仮原本」のデータ属性コードを持つデータに対しては編集を許可しないが、バージョンアップについては許可することとしている。このように、バージョンアップのみを許可することにより、以前のデータが失われず、電子データの編集履歴が分かるため、その証明力が高まることになる。

【0102】また、この原本性保証電子保存装置100では、「臍本」およびバックアップのデータについては、追記や編集を許可しない。その理由は、データの訂正や修正は、原本に対して施すべきものであり、コピーやバックアップに対して施すべきものではないからである。

【0103】また、新しいバージョンのデータ管理の仕方としては、新しいバージョンの内容を完全に記録する方式と、前バージョンとの差分のみを記録する方式とを選択できることとしている。なお、この差分のみを記録する差分モードでは、差分データを外部から渡すこととする。

【0104】図13は、図1に示した原本性保証電子保存装置100によるデータのバージョンアップ処理手順を示すフローチャートであり、図14は、この原本性保証電子保存装置100によるデータのバージョンアップ処理の概念を説明するための説明図である。

【0105】図13および図14に示すように、大容量

記憶媒体101がマウントされている場合には、保存データリストファイルを改ざん検知読み出し処理し（ステップS1301）、読み出した保存データリストから対象データのエントリを取得する（ステップS1302）。

【0106】そして、エントリの中からデータ属性MACを取得するとともに（ステップS1303）、対象データに対応したデータ属性情報ファイルからデータ属性MACを取得し（ステップS1304）、両属性MACが一致するか否かを確認する（ステップS1305）。

【0107】そして、両属性MACが一致しない場合には（ステップS1305否定）、エラー処理をおこなって（ステップS1317）処理を終了し、両属性MACが一致する場合には（ステップS1305肯定）、対象データに対応したデータ属性情報ファイルを改ざん検知読み出し処理する（ステップS1306）。

【0108】そして、読み出したデータ属性情報から最新バージョン番号を取得し（ステップS1307）、最新バージョン番号に1を加えて現バージョン番号とし

（ステップS1308）、外部から受け取ったデータをもとに現バージョンのバージョン属性情報作成処理をおこなう（ステップS1309）。たとえば、図14に示す例では、「Ver.2 1999.3.29 File#2.doc 102KB MAC」というバージョン2（Ver.2）のバージョン属性情報が作成される。

【0109】そして、現バージョンのバージョン属性情報をもとにデータ属性情報更新処理をおこなう（ステップS1310）。具体的には、新しいバージョン属性情報から作成日時情報を取得して最終更新日時情報とし、

データ属性情報の最終更新日時情報を新しい最終更新日時情報に更新し、データ属性情報に新しいバージョン属性情報を追加して新しいデータ属性情報とする。たとえば、図14に示す例では、「R00012321 原本 1999.3.27 1999.3.29 Ver.1 Ver.2 MAC」というデータ属性情報を作成する場合を示している。

【0110】そして、大容量記憶媒体101から保存データリストファイルを改ざん検知読み出し処理し（ステップS1311）、保存データリストから対象データに該当するエントリの内容を新しいデータ属性情報をもとに更新する（ステップS1312）。

【0111】そして、対象データのデータ名にバージョン番号を組み込んだファイル名でデータを大容量記憶媒体101にファイルとして保存し（ステップS1313）、新しいデータ属性情報を改ざん検知保存処理するとともに（ステップS1314）、新しい保存データリストを改ざん検知保存処理して（ステップS1315）、保存データリストファイルのメッセージ認証子（リストMAC）で内部記憶媒体104の媒体認証コードリストを更新して（ステップS1316）処理を終了する。

【0112】次に、図1に示した原本性保証電子保存装置100によるデータの編集処理について説明する。この原本性保証電子保存装置100では、「仮原本」および「原本」のデータについては修正履歴を残すことで証明力を高めるために、データに対する編集要求を拒否し、また「謄本」やバックアップは、本来編集すべき対象ではないので、同様に編集要求を拒否する。このため、結果的に「一般」のデータのみが編集可能となる。

【0113】図15は、図1に示した原本性保証電子保存装置100によるデータの編集処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体101がマウントされている場合には、保存データリストファイルを改ざん検知読み出し処理し(ステップS1501)、保存データリストから対象データに該当するエントリを取得する(ステップS1502)。

【0114】ここで、このエントリを取得できた場合には(ステップS1503肯定)、エラー処理をおこなって処理を終了し(ステップS1505)、エントリを取得できない場合には(ステップS1503否定)、対象データのデータファイルの編集を許容する(ステップS1504)。

【0115】次に、図1に示した原本性保証電子保存装置100へのクライアント(ホスト計算機110)からのログイン処理について説明する。この原本性保証電子保存装置100にデータを保存したりデータを読み出す前に、クライアントは原本性保証電子保存装置100にログインしなければならない。

【0116】このログイン処理としては、従来から知られているICカードを用いる技術を採用することもできるが、本実施の形態では、パスワードによる一般的なチャレンジレスポンス認証処理をおこなっている。なお、この原本性保証電子保存装置100は、内部記録媒体104のアカウント管理テーブルにあらかじめアカウント名とパスワードを記憶しており、外部システムがアクセスする場合には、外部システム用のアカウント名を使用し、原本の移動やコピーするために他の原本性保証電子保存装置にログインする際には、原本性保証電子保存装置用のアカウントを使用することとする。

【0117】図16は、図1に示した原本性保証電子保存装置100へのクライアントからのログイン処理手順を示すフローチャートである。同図に示すように、クライアントがアカウント名とログイン要求を送信し(ステップS1601)、原本性保証電子保存装置100が、このアカウント名とログイン要求を受信したならば(ステップS1602)、内部記録媒体104からアカウント管理テーブルを取得する(ステップS1603)。

【0118】そして、クライアントがアカウント名とパスワードを送信すると(ステップS1604)、原本性保証電子保存装置100では、アカウント管理テーブルから該当するパスワードを取得し(ステップS160

5)、該当するパスワードが存在しない場合には(ステップS1606肯定)、エラー処理をおこなって処理を終了する(ステップS1607)。

【0119】これに対して該当するパスワードが存在する場合には(ステップS1606否定)、乱数を生成してクライアントに送信する(ステップS1608～S1609)とともに、乱数とパスワードを合わせたものに對してハッシュ値を計算する(ステップS1610)。

【0120】一方、クライアントがこの乱数を受信したならば(ステップS1611)、乱数とパスワードを合わせたものに對してハッシュ値を計算し(ステップS1612)、計算したハッシュ値を送信する(ステップS1613)。

【0121】そして、原本性保証電子保存装置100が、このハッシュ値を受信したならば(ステップS1614)、両ハッシュ値を比較して両者が一致する場合には(ステップS1615肯定)、成功した終了コードを送信し(ステップS1616)、両者が一致しない場合には(ステップS1615否定)、エラー処理をおこなう(ステップS1618)。そして、クライアントがこの終了コードを受信(ステップS1617)した時点でログイン処理を終了する。なお、ステップS1607およびS1618のエラー処理時には、エラーを示す旨の終了コードをクライアントに送信する。

【0122】次に、図1に示した原本性保証電子保存装置100による日時の管理について説明する。この原本性保証電子保存装置100では、データアクセス履歴などに記録する日時は装置内部のタイマ105から取得するが、このタイマ105は設定変更が可能であるため、タイマ105を不正に変更することによりデータアクセス日時を偽ることが可能となる。

【0123】このため、本実施の形態では、タイマ105の設定をおこなうと図17(a)に示すように、タイマ設定履歴を自動的に内部記録媒体104に記憶するよう構成している。

【0124】ここで、タイマIDは、装置内部で自動的に付与されるシケンシャルな番号であり、タイマの設定を変更する都度番号が増える。また、データアクセス履歴に含まれる日時情報にはタイマIDも含まれる。

【0125】同図に示す場合に、タイマID=3において不正に日付を1月ずらし、その後タイマID=4で日付を戻していることが分かるため、データアクセス履歴の日時にタイマID=3の履歴が付されているデータは、不正に日時を偽ろうとした可能性があることが判明する。

【0126】また、原本性保証電子保存装置100から他の原本性保証電子保存装置へデータを移動したりコピーする場合にも、データアクセス履歴の日時に不都合が生じないようにするために、図17(b)に示すデータアクセス履歴をデータ属性情報に取り込む。なお、この

データアクセス履歴は、データ情報ファイルに記憶する。具体的には、同図に示す例では、移動先の原本性保証電子保存装置R010-0001055の日時19990217 10:13:43 ID=2が、移動元の原本性保証電子保存装置R010-0001032の日時19990217 10:10:21 ID=3に相当することができるため、移動したデータに不正が見つかった場合には、原本性保証電子保存装置をまたいで履歴を辿ることができる。

【0127】次に、図1に示した原本性保証電子保存装置100が用いる保存データリストファイル、データ属性情報ファイル、バージョン属性情報、媒体認証コードリスト、アカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例について図18および図19を用いて説明する。

【0128】図18(a)は、原本性保証電子保存装置100が用いる保存データリストファイルの一例を示す図であり、同図に示すように、この保存データリストファイルは、メッセージ認証子(リストMAC)と各リストエントリからなる。なお、ここで言う原本化とは、属性コードを「仮原本」から「原本」に変更することを意味する。そして、最初のリストMACを除いた部分が改ざん検知読み出し処理した際の保存データリストとなる。

【0129】図18.(b)は、原本性保証電子保存装置100が用いるデータ属性情報ファイルの一例を示す図であり、同図に示すように、このデータ属性情報ファイルは、メッセージ認証子(リストMAC)と属性管理データとからなる。そして、最初のデータ属性MACを除いた部分が改ざん検知読み出し処理した際のデータ属性情報となる。また、データ識別番号は、原本性保証電子保存装置識別番号(たとえば、R0010123)と、最新データ識別番号(たとえば、00000021)とをつなげたもの(R0010123-00000021)となる。

【0130】図18(c)は、原本性保証電子保存装置100が用いるバージョン属性情報の一例を示す図であり、同図に示すように、このバージョン属性情報は、メッセージ認証子(リストMAC)と、バージョン管理データと、各アクセス履歴とからなる。

【0131】図19(a)は、原本性保証電子保存装置100が用いる媒体認証リストコードの一例を示す図であり、同図に示すように、この媒体認証リストコードは、媒体識別番号およびメッセージ認証子(リストMAC)からなる複数の認証コードエントリにより形成される。

【0132】図19(b)は、原本性保証電子保存装置100が用いるアカウント管理リストの一例を示す図であり、同図に示すように、このアカウント管理リストは、アカウント名およびパスワードからなる各アカウントエントリからなる。なお、このアカウント管理リストは、任意の数のアカウントが登録できるような構造とし

ているが、最初から存在するクライアント用のアカウントや、原本性保証電子保存装置用のアカウントについては図示省略している。

【0133】図19(c)は、原本性保証電子保存装置100が用いる日時情報の内容を示す図であり、同図に示すように、この日時情報は、「年」、「月」、「日」、「時」、「分」、「秒」および「タイマID」からなる。

【0134】図19(d)は、原本性保証電子保存装置100が用いるタイマ設定履歴ファイルの内容を示す図であり、同図に示すように、このタイマ設定履歴ファイルは、設定前の日時情報、設定後の日時情報およびアカウント名からなる各タイマ設定履歴からなる。

【0135】

【発明の効果】以上説明したように、請求項1の発明によれば、複数の版によって形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のバージョンにまたがる原本性の保証を含む原本データの版管理を効率良くおこなうことができる。

【0136】また、請求項2の発明によれば、外部から電子データを原本として新規に保存する保存要求を受け付けた際に、所定の暗号鍵を用いて該電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報および所定のデータ識別情報を含むデータ属性情報を作成し、作成されたデータ属性情報を前記暗号鍵を適用して、該データ属性情報の改ざん検知情報を算定し、算定した改ざん検知情報をデータ属性情報に付与したデータと保存対象となる電子データとを記憶部に記憶することとしたので、改ざん検知情報を含むデータ属性情報を電子データとともに記憶することができる。

【0137】また、請求項3の発明によれば、外部から原本の電子データの読み出し要求を受け付けた際に、読み出し対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報に付与された改ざん検知情報と暗号鍵に応答する復号鍵に基づいて改ざんの有無を検証し、読み出されたデータ属性情報から読み出し対象となる版の版管理情報を記憶部から読み出し、読み出された版管理情報と復号鍵に基づいて改ざんの有無を検証し、読み出し対象となる電子データが改ざんされていないことが検証された場合に、該電子データを外部に提供することとしたので、改ざんを防止しつつ外部に電子データを提供することができる。

【0138】また、請求項4の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求を受け付けた際に、該バージョンアップの対象となる電子データのデータ属性情報を前記記憶部から読み出

し、読み出されたデータ属性情報と復号鍵とに基づいて改ざんの有無を検証し、新たな版の電子データに暗号鍵を適用して該新たな版の電子データの改ざん検知情報を算定し、算定された改ざん検知情報を含む版管理情報を作成し、作成された版管理情報を前記データ属性情報に追加する追加し、追加されたデータ属性情報に暗号鍵を適用して該データ属性情報の改ざん検知情報を算定し、算定された改ざん検知情報をデータ属性情報に付与したデータと新しい版の電子データとを記憶部に記憶することとしたので、改ざんを防止しつつ効率良くバージョンアップをおこなうことができる。

【0139】また、請求項5の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、該複製要求の対象となる電子データのデータ属性情報を記憶部から読み出し、読み出されたデータ属性情報を復号鍵を適用して、該データ属性情報の改ざんの有無を検証し、複製要求で指定された版の電子データを記憶部から読み出し、データ属性情報から指定された版の版管理情報を取り出し、取り出された版管理情報に復号鍵を適用して改ざんの有無を検証し、指定された版の電子データを指定された複製先に複製し、データ属性情報に含まれる属性情報を複写を示す情報に変更し、変更されたデータ属性情報を指定された複製先に複製することとしたので、改ざんを防止しつつ効率良く電子データを複製することができる。

【0140】また、請求項6の発明によれば、外部から保存される電子データが差分データである場合には、その版が差分データであることを示す版管理情報をデータ属性情報に含めて管理することとしたので、差分データとして電子データを管理する場合であっても効率良く版管理することができる。

【0141】また、請求項7の発明によれば、外部から原本となる電子データに対して版を指定した複製要求を受け付けた際に、複製対象となる版が差分データである場合には、該複製対象となる版よりも前の版で完全データを保持する版以上の電子データを複製することとしたので、差分データで電子データを管理する場合であっても、さらに効率良く版管理をおこなうことができる。

【0142】また、請求項8の発明に係る記録媒体は、前記請求項1～7のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項1～7の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図2】図1に示した原本性保証電子保存装置による新規データの保存処理手順を示すフローチャートである。

【図3】図1に示した原本性保証電子保存装置による新

規データの保存処理の概念を説明するための説明図である。

【図4】図1に示した大容量記憶媒体のマウント処理手順を示すフローチャートである。

【図5】図1に示した原本性保証電子保存装置によるデータ読み出し処理手順を示すフローチャートである。

【図6】図1に示した原本性保証電子保存装置による勝本作成処理手順を示すフローチャートである。

10 【図7】図1に示した原本性保証電子保存装置のデータ移動処理手順（移動先が同じ装置内である場合）を示すフローチャートである。

【図8】図1に示した原本性保証電子保存装置のデータ移動処理手順（移動先が他の装置内である場合）を示すフローチャートである。

【図9】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の転送受け入れ処理手順を示すフローチャートである。

【図10】図1に示した原本性保証電子保存装置によるデータの削除処理手順を示すフローチャートである。

20 【図11】図1に示した原本性保証電子保存装置によるデータ属性コードの変更態様を示す説明図である。

【図12】図1に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャートである。

【図13】図1に示した原本性保証電子保存装置によるデータのバージョンアップ処理手順を示すフローチャートである。

【図14】図1に示す原本性保証電子保存装置によるデータのバージョンアップ処理の概念を説明するための説明図である。

【図15】図1に示した原本性保証電子保存装置によるデータの編集処理手順を示すフローチャートである。

【図16】図1に示した原本性保証電子保存装置へのクライアントからのログイン処理手順を示すフローチャートである。

【図17】図1に示した原本性保証電子保存装置が用いるタイマ設定履歴およびアクセス履歴の一例を示す図である。

40 【図18】図1に示した原本性保証電子保存装置が用いる保存データリストファイル、データ属性情報ファイルおよびバージョン属性情報の一例を示す説明図である。

【図19】図1に示した原本性保証電子保存装置が用いる媒体認証コードリスト、アカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例を示す説明図である。

【符号の説明】

100 原本性保証電子保存装置

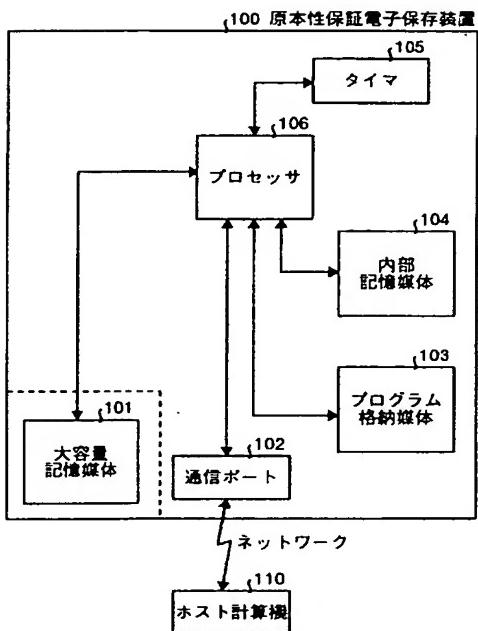
101 大容量記憶媒体

102 通信ポート

50 103 プログラム格納媒体

104 内部記録媒体
105 タイマ

【図1】

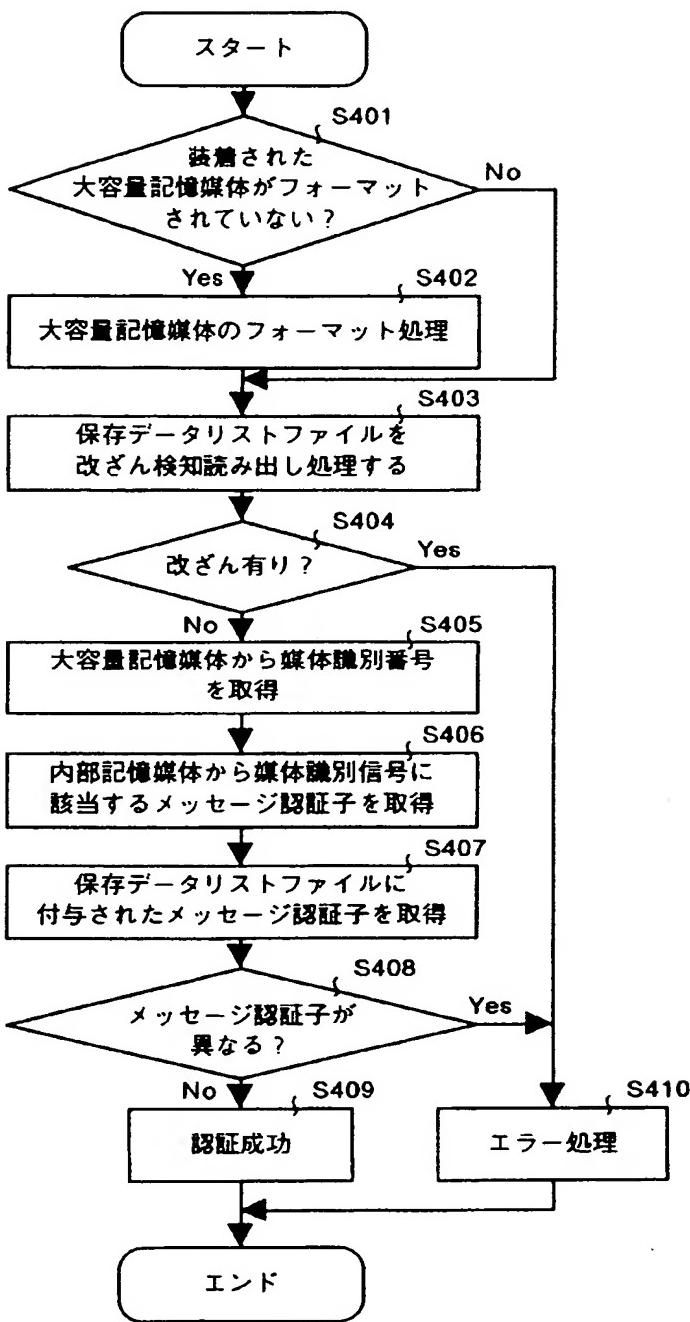


【図11】

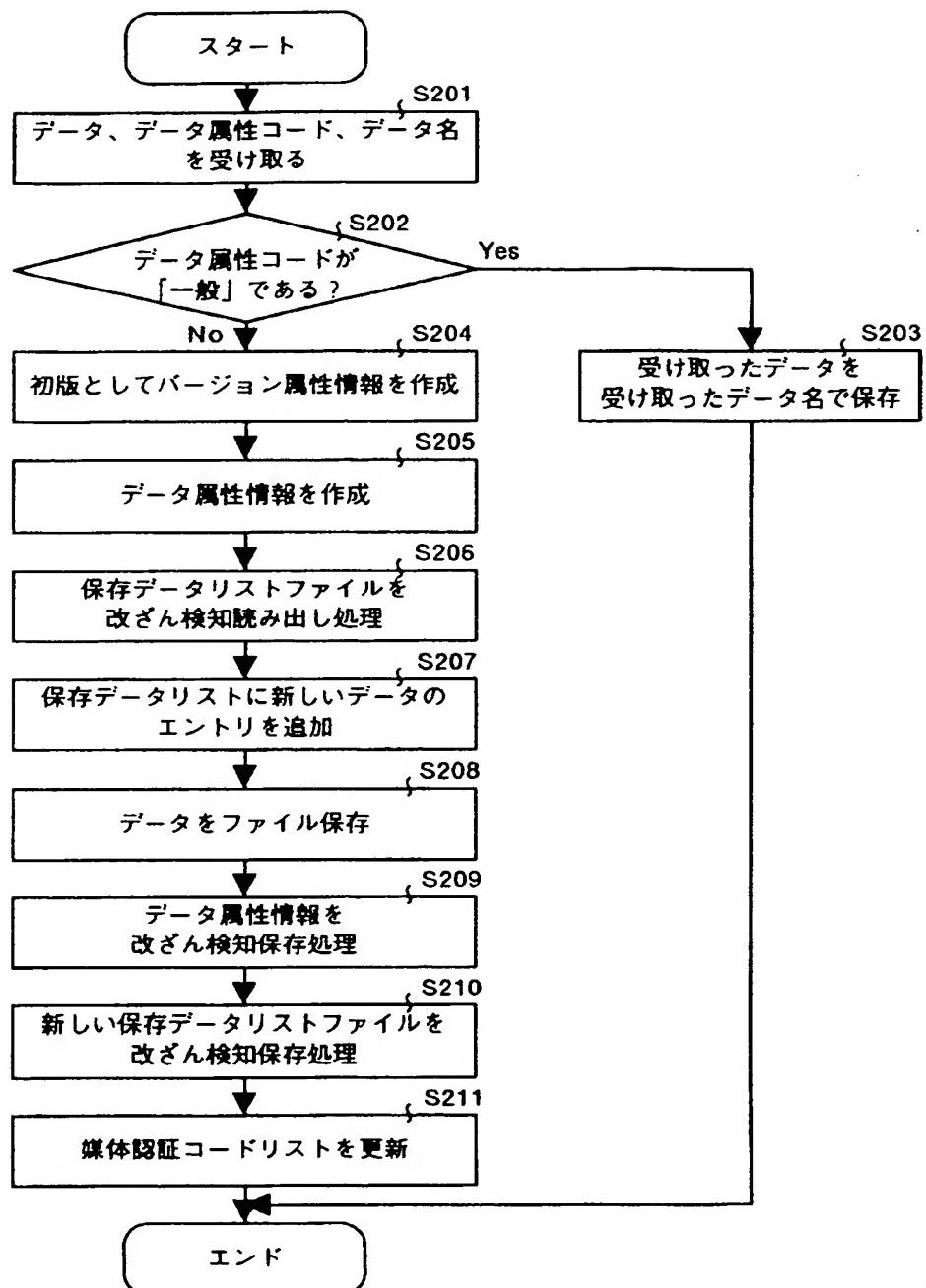
復旧前	復旧後
原本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ謄本	謄本

106 プロセッサ
110 ホスト計算機

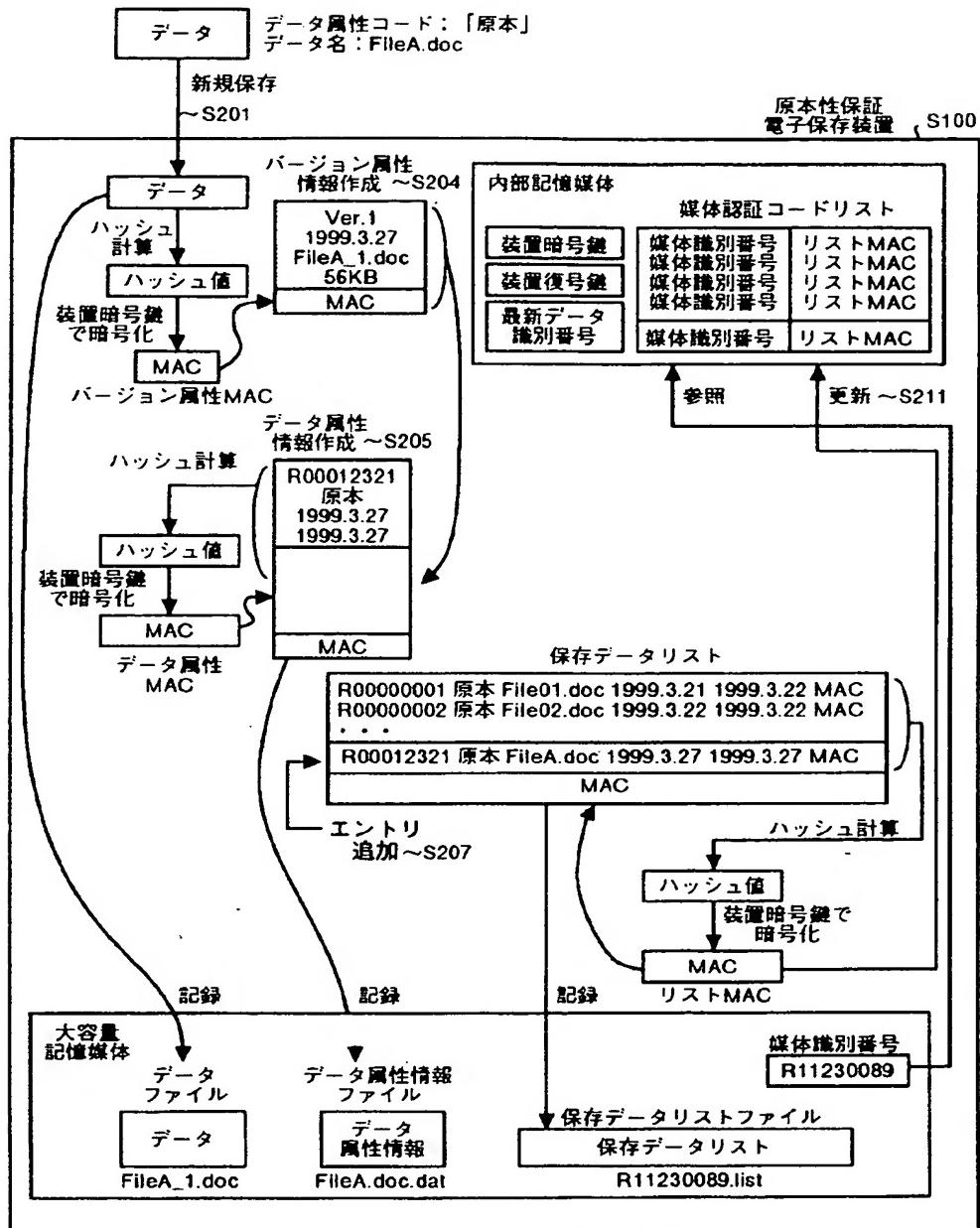
【図4】



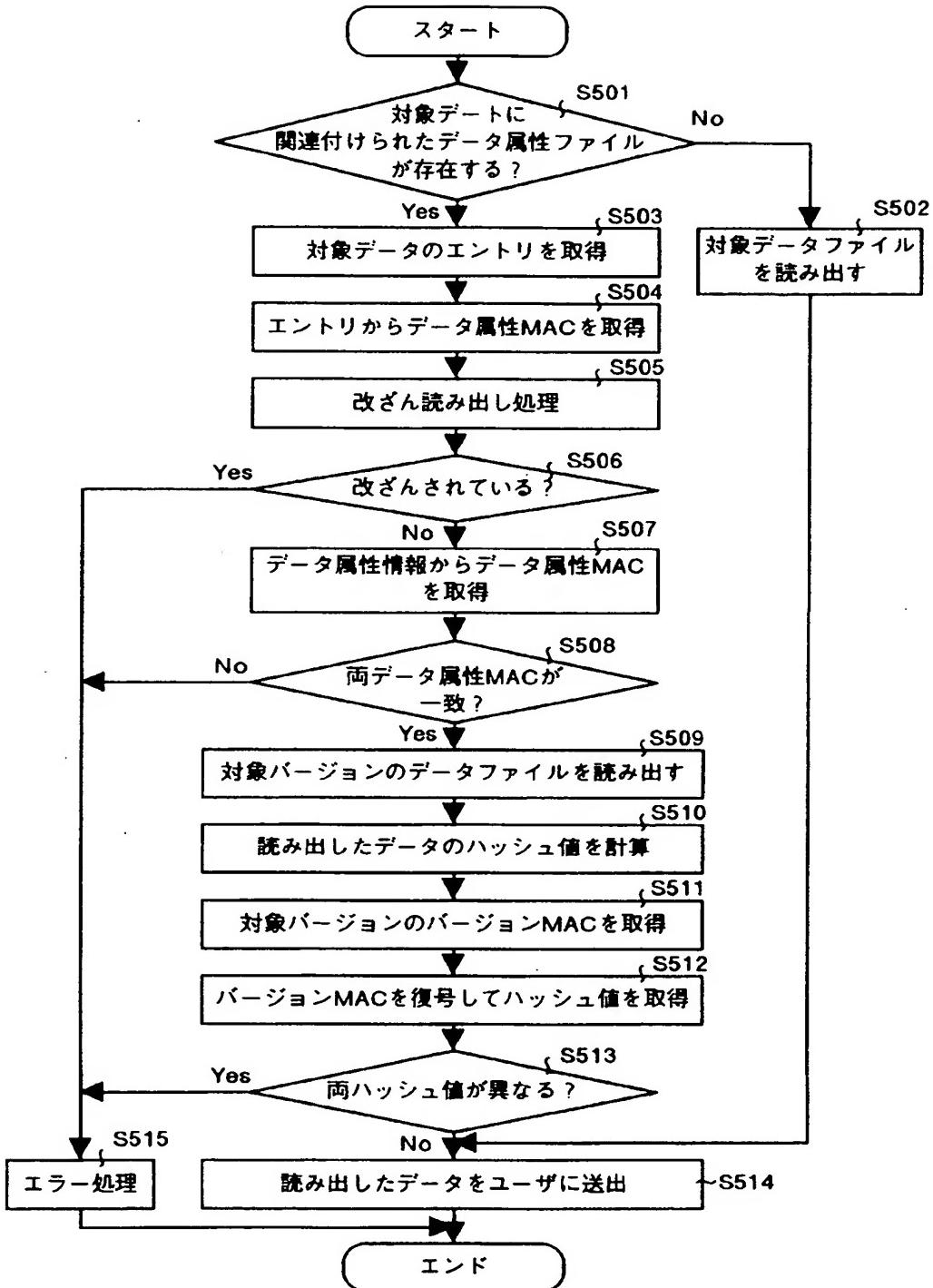
【図2】



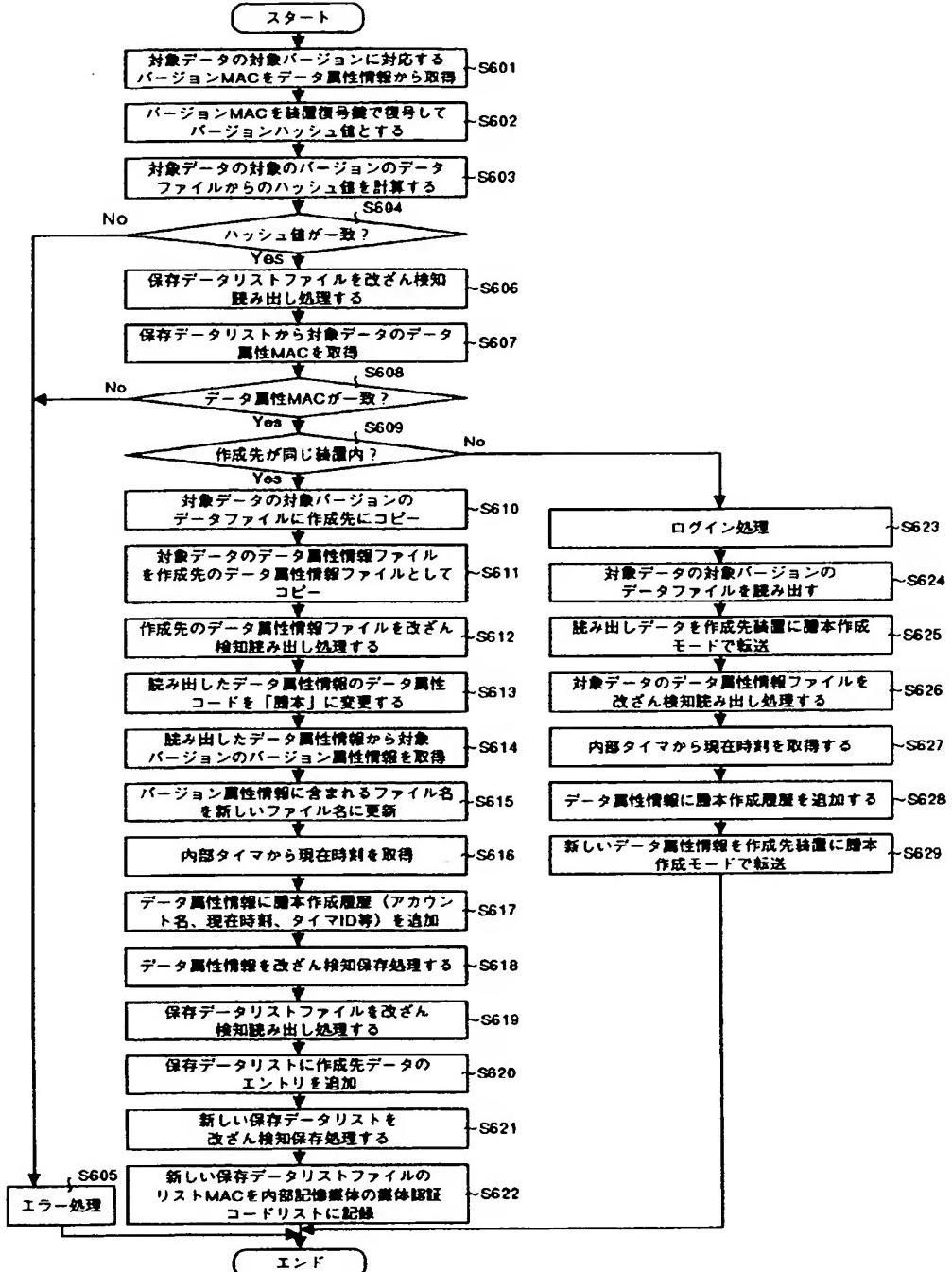
【図3】



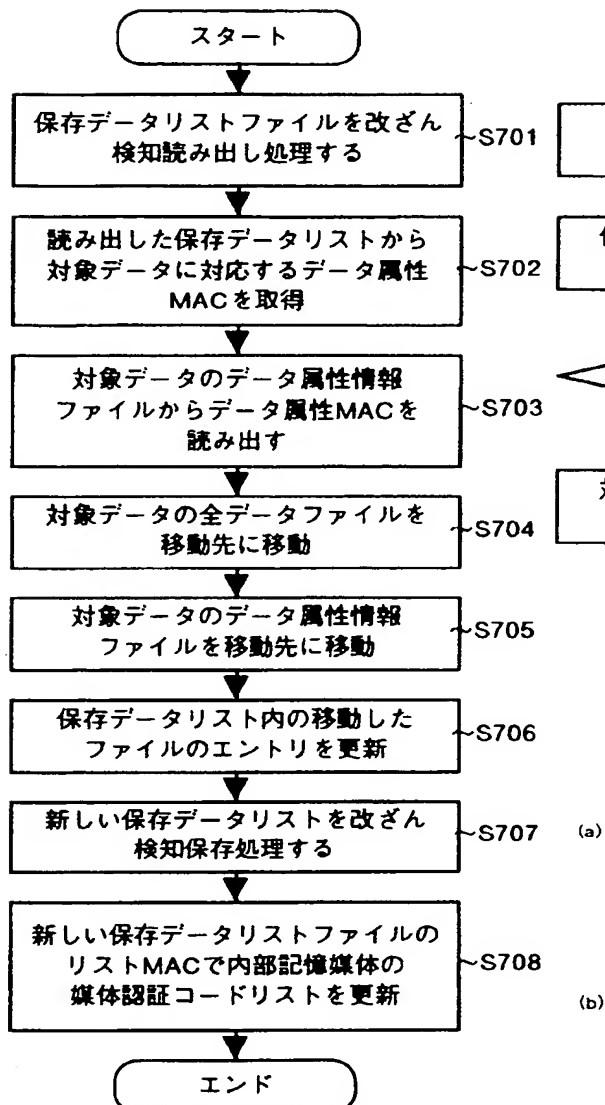
【図5】



【図6】



【図7】



【図17】

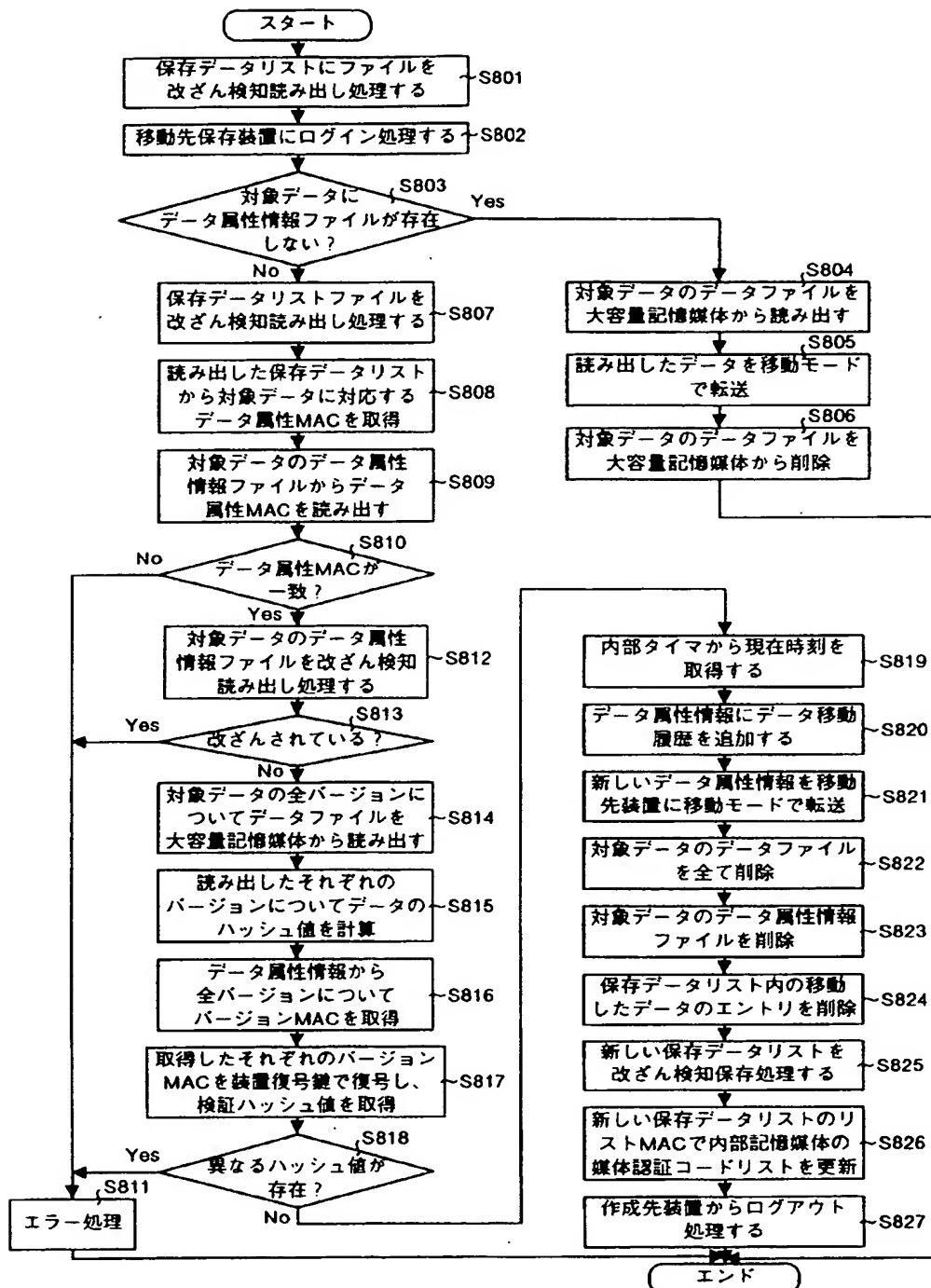
(a)

アクセス種別	アクセス日時	装置ID
CREATE	19990215 18:23:10 ID=1	R010-0001032
APPEND	19990215 18:23:30 ID=1	R010-0001032
MOVE TO	19990217 10:10:21 ID=3	R010-0001032
MOVE FROM	19990217 10:13:43 ID=2	R010-0001055

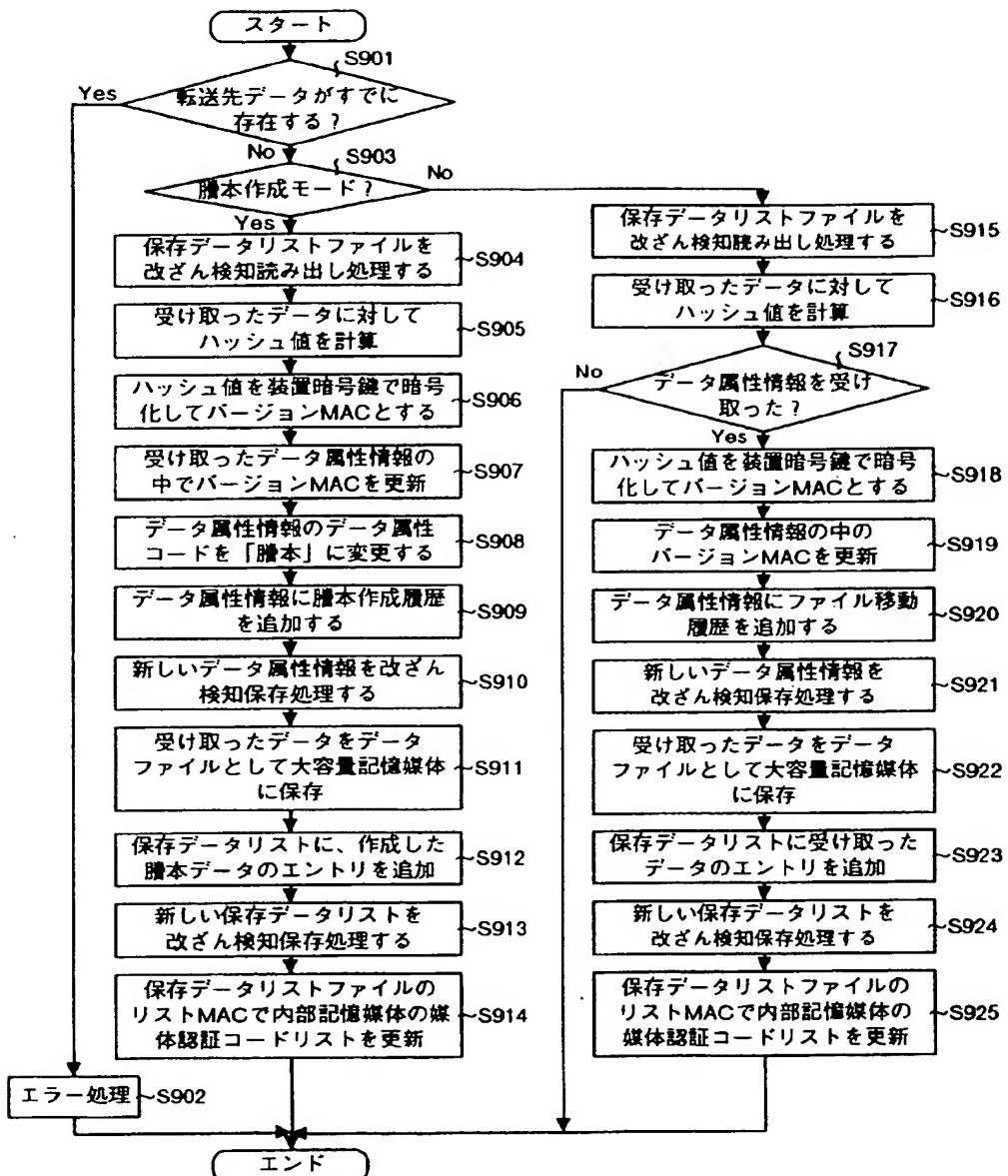
(b)

年	月	日	時	分	秒	タイマID
---	---	---	---	---	---	-------

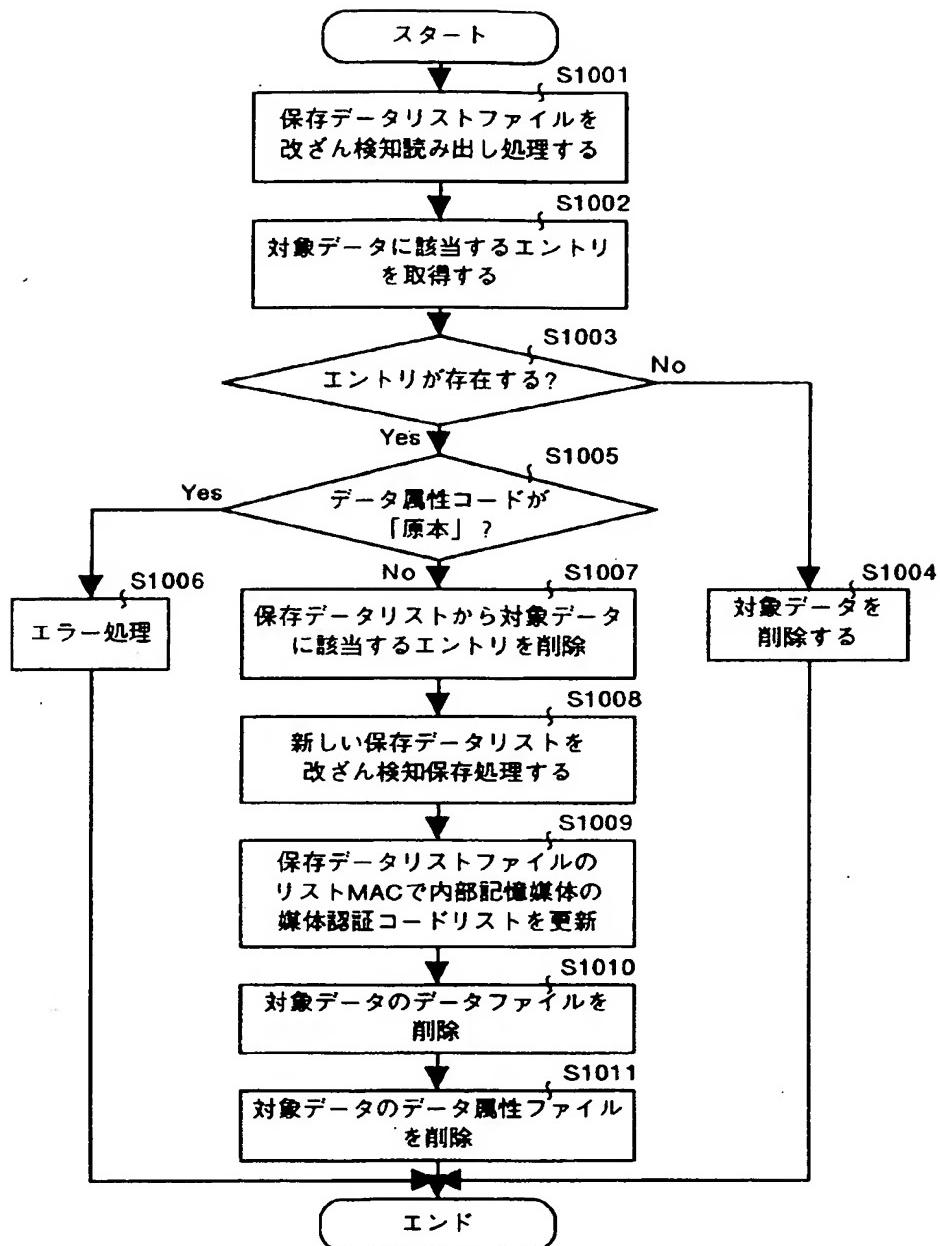
【図8】



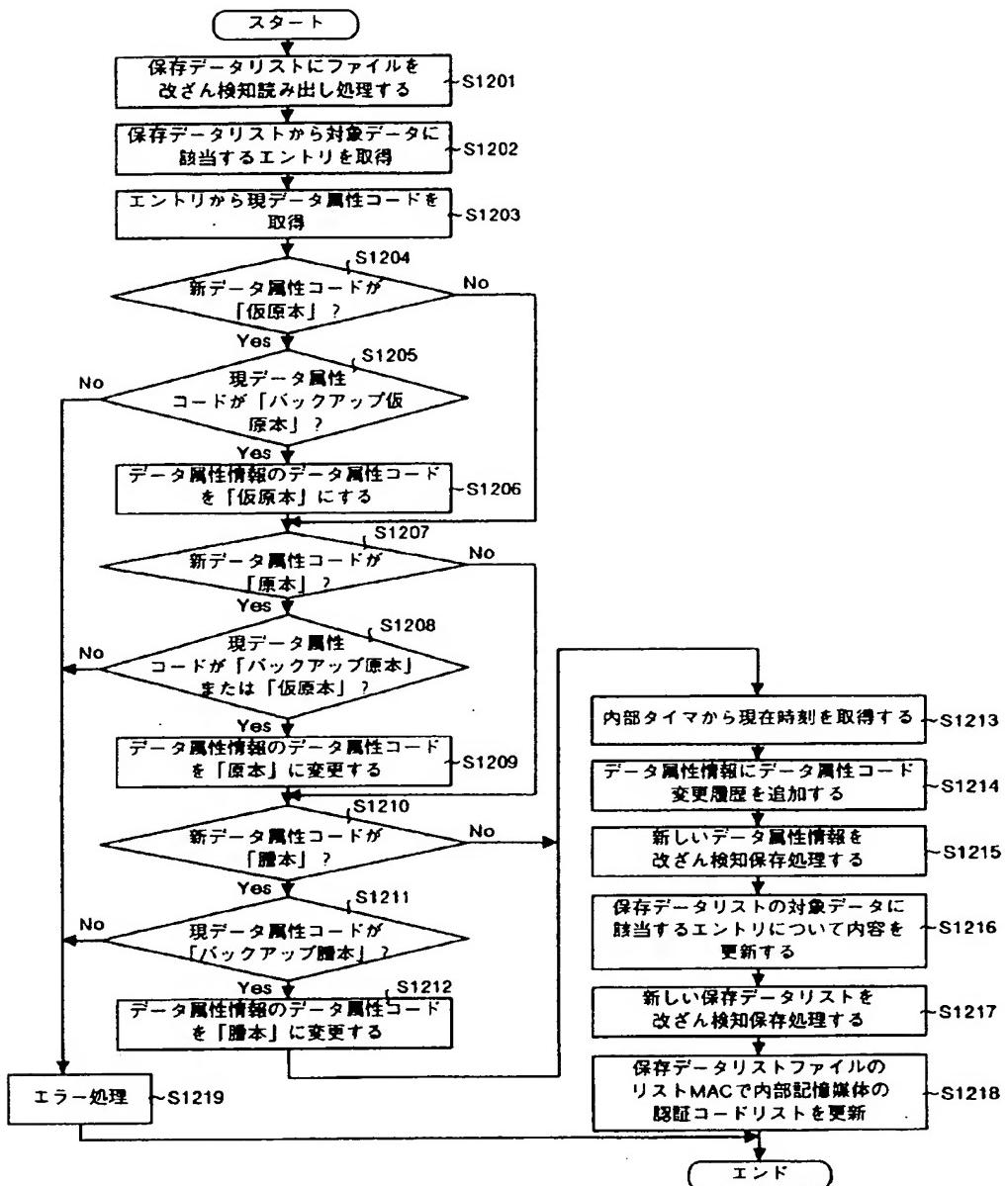
【図9】



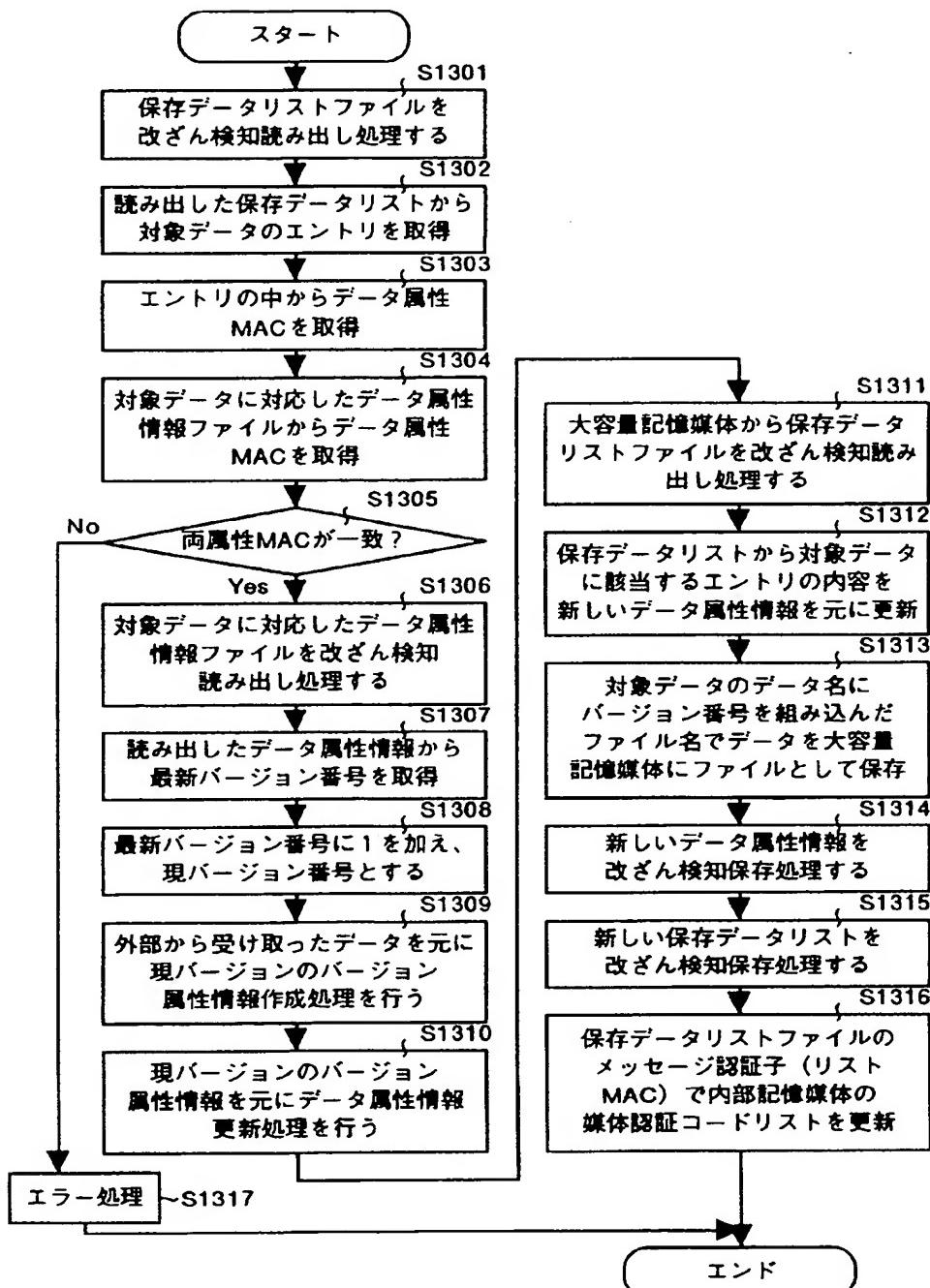
【図10】



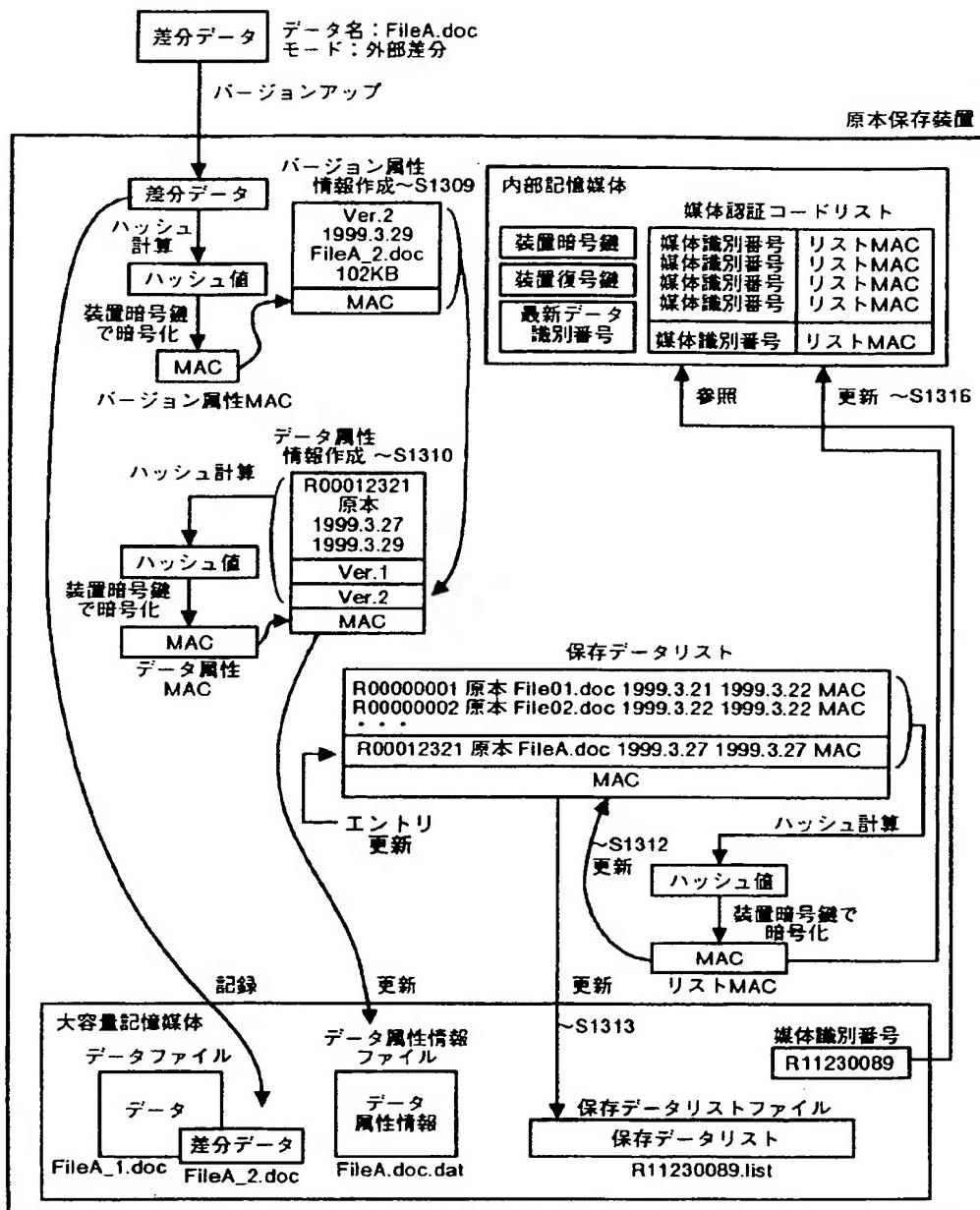
【図12】



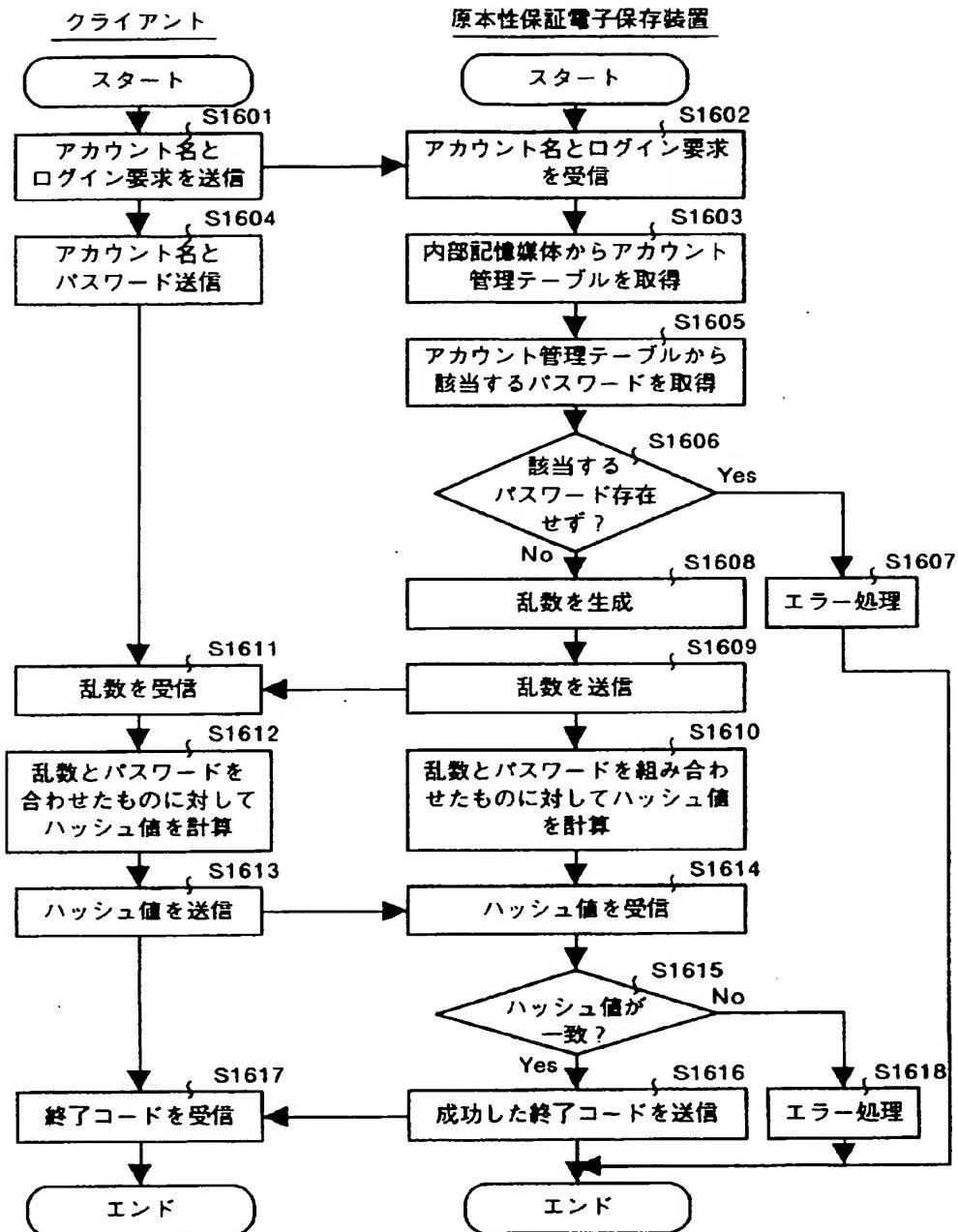
【図13】



【図14】



【図16】



【図18】

(a) メッセージ認証子 (リストMAC)

リストエントリ # 1	データ認識番号
	データ名
	フルパス名
	属性コード
	作成日時情報
	更新日時情報
	原本化日時情報
	メッセージ認証子 (データ属性MAC)
	リストエントリ # 2
リストエントリ # 3	リストエントリ # 3
	...

(b) メッセージ認証子 (リストMAC)

属性管理データ	データ認識番号
	データ名
	データ属性コード (原本、謄本、仮原本)
	作成日時情報
	最終更新日時情報
	最新バージョン番号
	バージョン属性情報 # 1
	バージョン属性情報 # 2
	...
	バージョン属性情報 # N

(c) メッセージ認証子 (バージョン属性MAC)

バージョン管理データ	バージョン番号
	データ属性コード (原本、謄本、仮原本)
	作成日時情報
	最終更新日時情報
	データファイルタイプ (完全、外部差分)
	データファイル名
	データファイルサイズ
アクセス履歴 # 1	アカウント名
	アクセス日時情報
	アクセス種別 (作成、原本化、参照)
	保存装置識別番号
アクセス履歴 # 2	アクセス履歴 # 2
	アクセス履歴 # 3
	...
アクセス履歴 # N	アクセス履歴 # N

フロントページの続き

F ターム(参考) 5B017 AA01 AA06 BA05 BA06 BA07
BB02 BB10 CA09 CA16
5J104 AA08 NA02 NA06 NA27 PA14
9A001 BB01 BB03 BB04 CC08 EE03
GG22 LL02 LL03